



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/905,342	07/14/2001	Markus Schmall	62434/RFJ/PT	3761
7590	07/28/2005		EXAMINER	
Richard F. Jaworski Cooper & Dunham LLP 1185 Avenue of the Americas New York, NY 10036			FIELDS, COURTNEY D	
			ART UNIT	PAPER NUMBER
			2137	

DATE MAILED: 07/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/905,342	SCHMALL ET AL.	
	Examiner	Art Unit	
	Courtney D. Fields	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 21 April 2005.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-19 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-19 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-19 are pending.

Response to Arguments

2. Applicant's arguments filed 21 April 2005 have been fully considered but they are not persuasive.
3. Referring to the rejection of claim 1, the Applicant contends and argues that the prior art Nachenberg does not teach nor suggest heuristically analyzing a subject file to generate a set of flags along with statistical information, using the set of flags with statistical information to perform at least one search for a scan string and/or a statement type in the subject file, and triggering a positive detection alarm if each of the at least one search is found at least a corresponding predetermined number of times. The Examiner disagrees and asserts that Nachenberg does teach a method for detecting a class of viral code using a polymorphic virus detection module. The polymorphic anti-virus module heuristically analyze and emulate the data file for viruses until the system determines if the data file is not a virus and whether the file is data file or an executable file. (See Column 2, lines 51-67 and Column 3, lines 37-53) The polymorphic anti-virus module comprises a dynamic exclusion module which examines the statistical information (instruction/interrupt usage profiles) of each known polymorphic virus. The emulation control module fags theses viruses after performing at least one search for a scan string or statement type within the data file (See Column 3, lines 37-53 and Column 11, lines 3-22) and triggering a positive detection if at least one search is found

reducing the number of instructions emulated prior to scanning the target files (See Column 3, lines 44-53)

4. Therefore the rejection of claims 1-19 are maintained in view of the reasons above and in view of the reasons below.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-19 are rejected under 35 U.S.C. 102(b) as being anticipated by Nachenberg (US Patent No. 5,826,013).

Regarding claim 1, Nachenberg teaches a method of detecting a class of viral code, comprising:

heuristically analyzing a subject file to generate a set of flags along with statistical information (col.3, lines 37-53);

using the set of flags with statistical information to perform at least one search for a scan string and/or a statement type in the subject file (col.3, lines 37-53 and col.11 lines 3-22);

and triggering a positive detection alarm if each of the at least one search is found at least a corresponding predetermined number of times (col.3, lines 44-46).

Regarding claim 2, Nachenberg teaches the subject file includes source code in a predetermined programming language (col.3, lines 17-35).

Regarding claim 3, Nachenberg teaches the predetermined programming language is a script language (col.5, lines 11-50).

Regarding claim 4, Nachenberg teaches the subject file includes a file for a predetermined word processor (col.11, lines 35-53).

Regarding claim 5, Nachenberg teaches at least one flag in the set of flags corresponds to a copy operation associated with one of the lass of viral code (col. 1, lines 18-24 and col.3 lines 37-53).

Regarding claim 6, Nachenberg teaches at least one flag in the set of flags corresponds to an operation for adding data from a string to a target module (col.5, lines 11-50).

Regarding claim 7, Nachenberg teaches at least one flag in the set of flags corresponds to an operation for importing another code (col.3, lines 37-53).

Regarding claim 8, Nachenberg teaches at least one flag in the set of flags corresponds to an operation for disabling virus protection features in a target application (col.5, lines 5-8).

Regarding claim 9, Nachenberg teaches the searched statement type corresponds to an operation for disabling functionalities in a target application (col.4, lines 66-67 and col. 5, lines 1-10).

Regarding claim 10 (claim 12 as written), Nachenberg teaches the searched statement type corresponds to an operation for overwriting system macros (col.4, lines 3-14).

Regarding claim 11 is a program storage device claim that is substantially equivalent to

method claim 1 , therefore claim 11 is rejected for the same reasons.

Regarding claim 12 is a system claim that is substantially equivalent to method claim 1,

therefore claim 12 is rejected for the same reasons.

Regarding claim 13 is a computer data signal claim that is substantially equivalent to

method claim 1 , therefore claim 13 is rejected for the same reasons.

Regarding claim 14 is an apparatus claim that is substantially equivalent to method claim 1 ,

therefore claim 14 is rejected for the same reasons.

Regarding claim 15, Nachenberg teaches the heuristic analyzer is rule-based and comprises a heuristic engine and heuristic rules (col.1, lines 63-67 and col.10 lines 28-43).

Regarding claim 16, Nachenberg teaches the heuristics engine, using the heuristic rules, parses the subject file (col.1, lines 63-67, col.3, lines 1-24, and col.10 lines 28-43).

Regarding claim 17, Nachenberg teaches the heuristic rules include sets of heuristic flags stored in a rules table (col.3, lines 9-23).

Regarding claim 18, Nachenberg teaches the search component is rule-based

and comprises a search engine and viral code class rules (col.3, lines 1-23 and col.4 lines 23-41).

Regarding claim 19, Nachenberg teaches the search component is a neural network (fig.2, col.6, lines 41-67 and col.7, lines 1- 8).

Conclusion

3. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Courtney D. Fields whose telephone number is 571-272-3871. The examiner can normally be reached on Mon - Thurs. 6:00 - 4:00 pm; off every Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2137

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

CO9
cdf
July 20, 2005

Matthew Smithers
MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137